Project: forge a signature to pretend that you are Satoshi

代码说明：首先是 ECDSA 签名算法的代码，接下来利用课件的方法编写代码对 Satoshi 的签名进行伪造，假设已知他的一个签名，之后可在不知晓他私钥的前提下伪造出一个对 e'的签名（r',s'）。具体代码则将课件数学式子转化为代码即可。

运行说明：直接运行 py 文件

运行结果：